

سوتریا: شناسایی کانال‌های فرمان و کنترل پنهان مبتنی بر شبکه‌های اجتماعی در بات‌نت‌های نسل جدید

منصوره قنادی^۱، مهدی آبادی^۲

^۱ گروه مهندسی کامپیوتر، دانشکده تحصیلات تکمیلی، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران
ghanadi.mansoureh@gmail.com

^۲ استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران
abadi@modares.ac.ir

چکیده

امروزه بات‌نت‌ها به یکی از جدی‌ترین تهدیدات در فضای اینترنت تبدیل شده‌اند. در هر بات‌نت از یک بستر ارتباطی با نام کانال فرمان و کنترل برای هدایت میزبان‌های آلوده به بات استفاده می‌شود. از آن‌جا که با شناسایی کانال‌های فرمان و کنترل به آسانی می‌توان بات‌نت‌های مختلف را متلاشی کرد، شناسایی این کانال‌ها در روش‌های تشخیص بات‌نت از اهمیت زیادی برخوردار است. مهاجمین با هدف افزایش طول عمر بات‌نت‌های خود از استراتژی‌های متفاوتی برای ایجاد کانال‌های فرمان و کنترل استفاده می‌کنند. در سال‌های اخیر، شبکه‌های اجتماعی به دلیل دارا بودن میلیون‌ها کاربر فعال مورد توجه مهاجمین قرار گرفته‌اند، به طوری که انواع مختلفی از بات‌نت‌های نسل جدید مبتنی بر شبکه‌های اجتماعی معرفی شده است. در این مقاله، روشی با نام سوتریا برای تشخیص بات‌نت‌های نسل جدیدی پیشنهاد می‌شود که از نهان‌نگاری در تصاویر اشتراکی کاربران شبکه‌های اجتماعی برای ایجاد کانال‌های فرمان و کنترل پنهان استفاده می‌کنند. در روش پیشنهادی با بررسی تصاویر اشتراکی در شبکه اجتماعی فعالیت‌های گروهی مشکوک به بات کاربران در دوره‌های زمانی متفاوت شناسایی شده و میزان شهرت منفی هر کاربر با توجه به سابقه و شباهت فعالیت‌های گروهی مشکوک به بات وی محاسبه می‌شود. در نهایت کاربران با شهرت منفی بالا به عنوان کاربران آلوده به بات گزارش می‌شوند. نتایج آزمایش‌ها نشان می‌دهند که روش سوتریا قادر است کانال‌های فرمان و کنترل پنهان مبتنی بر شبکه‌های اجتماعی را با نرخ هشدار نادرست پایین شناسایی کند.

کلمات کلیدی

تشخیص بات‌نت، شبکه اجتماعی، کانال فرمان و کنترل، کانال پنهان، نهان‌نگاری، نهان‌کاوی، شهرت منفی.

۱- مقدمه

است. برای مقابله با این روش‌ها، مدیران بات به طور پیوسته استراتژی‌های خود برای ایجاد کانال‌های فرمان و کنترل را تغییر می‌دهند [۲].

هر شبکه اجتماعی شامل مجموعه‌ای از موجودیت‌ها (از قبیل کاربران در محیط‌های مجازی) و وابستگی‌های اجتماعی (از قبیل روابط دوستی) میان آن‌ها است. شبکه‌های اجتماعی برخط (OSNs) را می‌توان به عنوان یکی از جدیدترین سرویس‌های اینترنتی در نظر گرفت که شکل جدیدی از برقراری ارتباط و به اشتراک‌گذاری اطلاعات را در اینترنت فراهم می‌کنند.

هر بات‌نت^۱ شامل گروهی از میزبان‌هایی است که به کد مخرب^۲ یکسان آلوده شده و توسط یک بستر ارتباطی با نام کانال فرمان و کنترل (C&C) هدایت می‌شوند [۱]. امروزه از بات‌نت‌ها برای انجام فعالیت‌های غیرقانونی از قبیل ارسال هرزنامه، حمله‌های جلوگیری از سرویس توزیعی و سرقت اطلاعات محرمانه استفاده می‌شود. در سال‌های اخیر روش‌های متعددی برای تشخیص بات‌نت‌ها مبتنی بر شناسایی ترافیک کانال‌های فرمان و کنترل پیشنهاد شده